

## ABSTRACT

A method and apparatus for providing verifiable digital signatures. In one embodiment, a method includes converting, on a computer system, digital data representative of a document into a predetermined format, and applying the 5 predetermined format and a viewer program to a hash function to mathematically operate on the predetermined format and the viewer program and provide a message digest. The viewer program is used for viewing the predetermined format that is a representation of the document. The method further includes encrypting the message digest using a private key to provide a digital signature. In one embodiment, the 10 predetermined format is a bitmap representation of the document. Moreover, in one embodiment, the method further includes incorporating a file in the digital signature, where the file includes one or more parameters specifying an environment of the computer system at the time of creation of the digital signature. The method and apparatus establishes integrity and trust in digital signatures, providing evidence that 15 the sending and receiving parties are seeing the identical view of the digitally signed document(s).